BILL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,634	09/07/2000	Babak Tehranchi	81399N-R	1654

1333 7590 12/06/2004

PATENT LEGAL STAFF
EASTMAN KODAK COMPANY
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/656,634	TEHRANCHI, BABAK	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 19 August 2004 have been fully considered but they are not persuasive. Applicant's argument that the Warren reference does not disclose encryption keys being synchronized with different blocks is not persuasive because Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56). The encryption keys are provided to the encryptor (Fig. 16) and tags are provided during the encoding process for synchronization purposes (Col. 9, lines 40-48).

2. Applicant's argument that the Warren reference does not disclose that the data blocks are different sizes is not persuasive because that claim limitation is found in claim 60, which was rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Shukla, U.S. Patent No. 6,345,101. Warren does not disclose that the data blocks can be different sizes. Shukla discloses a cryptographic method for data communications wherein the data blocks communicated can be of different sizes (Col. 2, lines 52-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the data blocks of Warren to be different sizes in order to avoid the use of many standard techniques used in encryption methods as taught in Shukla (Col. 2, lines 48-53).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-10, 12, 13, 15-18, 20-41, 43, 44, 47-49, 51, 52, 57-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Warren, U.S. Patent No. 5,963,909. Referring to claims 1, 3, 4, 12, 15, 17, 20-24, 26-30, 32-37, 39-41, 43, 47-49, 51, 57-59, Warren discloses a copy management system for multi-media wherein multi-media is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption engine that, for each said single data block, producing an encrypted data block using said encryption key from said encryption key generator. The encryption keys are provided to the encryptor (Fig. 16) and tags are provided during the encoding process for synchronization purposes (Col. 9, lines 40-48), which meets the limitation of encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block. The data is transmitted over its own channel (Fig. 13, Abstract), which meets the limitation of a data transmission channel for delivering said encryption key from said encryption key generator engine of the digital data receiver. The encryption keys can be transmitted separately from the data (Abstract), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. The tag information used for synchronization is also transmitted separately (Col. 9, lines 40-65), which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver.

Referring to claim 2, Warren discloses that the receiver of the encrypted data decrypts with the encryption keys (symmetric) at the decryptor (Fig. 17), which meets the limitation of digital data receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption.

Referring to claim 5, Warren discloses that the communication channel can be a satellite channel (Col. 1, lines 22-24), which meets the limitation of data transmission channel is a wireless transmission network.

Referring to claim 6, Warren discloses that the commnication channel can be a telephone network (Col. 6, line 40), which meets the limitation of a data transmission channel that utilizes dedicated phone service.

Referring to claims 7, 13, 16, Warren discloses that the communication network uses a portable storage medium (Col. 1, lines 10-15).

Referring to claims 8-10, Warren discloses that the communication network can be cable networks, The Internet, which meets the limitation of a wide area network, or intranets, which meets the limitation of a local area network (Col. 1, lines 22-23).

Referring to claim 18, Warren discloses that the tags used for synchronization are generated using pseudo-random sequences (Col. 2, lines 36-47).

Referring to claims 25, 31, Warren discloses that the channel that the encryption keys and synchronization data are distributed on can be encrypted (Col. 16, lines 16-24 & Fig. 12).

Referring to claim 38, Warren discloses that NULL keys can be used to created unencrypted data blocks (Col. 14, lines 18-21), which meets the limitation of padding said plurality of encryption keys using dummy bits.

Referring to claims 44, 52, Warren discloses that the compression can be done using MPEG compression methods (Col. 5, line 4).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 11, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Handelman, U.S. Patent No. 5,774,546. Referring to claims 11, 14, Warren discloses a copy management system for multi-media wherein multi-media is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption engine that, for each said single data block, producing an encrypted data block using said encryption key from said encryption key generator. The encryption keys are provided to the encryptor (Fig. 16) and tags are provided during the encoding process for synchronization purposes (Col. 9, lines 40-48), which meets the limitation of encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block. The data is transmitted over its own channel (Fig. 13, Abstract), which meets the limitation of a data transmission channel for delivering said encryption key from said encryption key generator engine of the digital data receiver. The encryption keys can be transmitted separately from the data (Abstract), which

meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. The tag information used for synchronization is also transmitted separately (Col. 9, lines 40-65), which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose using smart cards in the copy management system. Handelman discloses a data access system wherein video data is accessed using a smart card that communicates seeds, keys, and access control algorithms with the video decoder (Col. 2, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use smart cards in the copy management system of Warren in order to provide secure access to restricted means as taught in Handelman (Col. 1, line 18).

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Schneier. Referring to claim 19, Warren discloses that the tags used for synchronization are generated using pseudo-random sequences (Col. 2, lines 36-47). Warren does not disclose that linear feedback shift registers can generate the pseudo-random sequences. Schneier discloses that pseudo-random sequences can be generated using linear feedback shift registers (Page 373). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the pseudo-random sequences of Warren to be generated using a linear feedback shift register because shift registers have been used to generate stream ciphers since the beginning of electronics as taught in Schneier (Page 372).

8. Claims 42, 45, 46, 50, 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Chaum, U.S. Patent No. 5,959,717.

Referring to claims 42, 50, Warren discloses a copy management system for multi-media wherein multi-media is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption engine that, for each said single data block, producing an encrypted data block using said encryption key from said encryption key generator. The encryption keys are provided to the encryptor (Fig. 16) and tags are provided during the encoding process for synchronization purposes (Col. 9, lines 40-48), which meets the limitation of encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block. The data is transmitted over its own channel (Fig. 13, Abstract), which meets the limitation of a data transmission channel for delivering said encryption key from said encryption key generator engine of the digital data receiver. The encryption keys can be transmitted separately from the data (Abstract), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. The tag information used for synchronization is also transmitted separately (Col. 9, lines 40-65), which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose that the video signal can be decoded at a projector. Chaum discloses a copy protection system that utilizes two video parts in combination at the projector to view the film (Col. 1, line 46 – Col. 2, line 54). It would have been obvious to one of ordinary skill in the art at the time the invention was made

for the decoder of Warren to be housed in a projector because film projection systems are the dominate way to publicly screen motion pictures as taught in Chaum (Col. 1, lines 12-14).

Referring to claims 45, 46, 53-56, Warren does not disclose that the video signal is encrypted based on color data. Chaum discloses that rather than performing frame by frame protection of the film, protection can be performed on a color basis (Col. 5, lines 14-17). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the video data of Warren with respect to color in order to produce holes in the video content so that theft or piracy would be less desirable as taught in Chaum (Col. 5, lines 16-30).

9. Claims 60, 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Shukla, U.S. Patent No. 6,345,101. Referring to claims 60, 61, Warren discloses a copy management system for multi-media wherein multi-media is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption engine that, for each said single data block, producing an encrypted data block using said encryption key from said encryption key generator. The encryption keys are provided to the encryptor (Fig. 16) and tags are provided during the encoding process for synchronization purposes (Col. 9, lines 40-48), which meets the limitation of encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks and a block synchronization index indicating a correspondence between said encryption key and said single data block. The data is transmitted over its own channel (Fig. 13, Abstract), which meets the limitation of a data transmission channel for delivering said encryption key from said encryption key generator engine of the digital data

receiver. The encryption keys can be transmitted separately from the data (Abstract), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. The tag information used for synchronization is also transmitted separately (Col. 9, lines 40-65), which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose that the data blocks can be different sizes. Shukla discloses a cryptographic method for data communications wherein the data blocks communicated can be of different sizes (Col. 2, lines 52-65). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the data blocks of Warren to be different sizes in order to avoid the use of many standard techniques used in encryption methods as taught in Shukla (Col. 2, lines 48-53).

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

THOMAS R. PEESO
PRIMARY EXAMINER